Amendments to the Claims

1. (ORIGINAL) A method for calculating the product P of a first number X and a second number Y, modulo N, where Y is partitioned into j words each of length p bits, and X has a length (m + n) bits, comprising the steps of:

a) initialising a product register, P

b) loading a first one of the j words of Y into a multiplier;

c) multiplying the loaded word of Y by X to form an intermediate product T;

d) updating the product register P with the sum of T and $P * 2^p$;

e) reducing the contents of the product register P by subtraction of a value P_H (N' / 2);

f) loading a successive one of the j words of Y into the multiplier and repeating steps c) to e) for each one of the j words of Y,

wherein N' is an integer multiple of N, and the value N' is selected such that the (m – 1) most significant bits are equal to '1', and the least significant bit is '0', and

wherein P_H is selected as the (p + 2) most significant bits of P in the register.

2. (ORIGINAL) The method of claim 1 in which the second number Y is also (m + n) bits in length.

3. (CURRENTLY AMENDED) The method of claim 1 ~~or claim 2~~ further including the step of selecting $m \geq p + 3$.

4. (CURRENTLY AMENDED) The method of ~~any preceding claim~~claim 1 further including the step of selecting (m + n) as a multiple of p bits.

5. (CURRENTLY AMENDED) The method of claim 1~~any preceding claim~~ further including the step of using a (p + 2) * p multiplier to perform the multiplying step and for deriving the value P_H (N' / 2).

6. (CURRENTLY AMENDED) The method of claim 1~~any preceding claim~~ in which the first one of the j words of Y loaded into the multiplier is the most

significant word, and successive ones of the j words are loaded in decreasing order of significance.

7. (CURRENTLY AMENDED) The method of claim 1~~any preceding claim~~ carried out in a pipelined processing architecture, in which the multiplication step for a successive cycle through steps c) to e) commences prior to completion of the subtraction step e) of a preceding cycle.

8. (ORIGINAL) A processor for calculating the product P of a first number X and a second number Y, modulo N, where Y is partitioned into j words each of length p bits, and X has a length (m + n) bits, comprising:

a) initialisation means for initialising a product register, P

b) loading means for loading a first one of the j words of Y into a multiplier;

c) a multiplier for multiplying the loaded word of Y by X to form an intermediate product T;

d) update means for updating the product register P with the sum of T and $P * 2^p$;

e) reduction means for reducing the contents of the product register P by subtraction of a value $P_H (N' / 2)$;

f) control means for loading successive ones of the j words of Y into the multiplier and repeating the functions of the multiplier, the update means and the reduction means for each one of the j words of Y,

wherein N' is an integer multiple of N, and the value N' is selected such that the (m – 1) most significant bits are equal to '1', and the least significant bit is '0', and

wherein P_H is selected as the (p + 2) most significant bits of P in the register.

9. (ORIGINAL) The processor of claim 8 in which the second number Y is also (m + n) bits in length.

10. (CURRENTLY AMENDED) The processor of claim 8 ~~or claim 9~~ in which $m \geq p + 3$.

11. (CURRENTLY AMENDED) The processor of ~~any one of claims 8 to 10~~ claim 8 in which (m + n) is an integer multiple of p bits.

12. (CURRENTLY AMENDED) The processor of ~~any one of claims 8 to 11~~ claim 8 in which the multiplier is a (p + 2) * p multiplier also adapted to provide the value of P_H (N' / 2) to the reduction means.

13. (CURRENTLY AMENDED) The processor of ~~any one of claims 8 to 12~~ claim 8 in which the loading means is adapted to load the most significant word of Y as the first one of the j words of Y loaded into the multiplier, and successive ones of the j words are loaded in decreasing order of significance.

14. (CURRENTLY AMENDED) The processor of ~~any one of claims 8 to 13~~ claim 8 implemented in a pipelined processing architecture, in which the multiplier commences the multiplication operation to obtain a new value of T for a successive cycle prior to the reduction means completing the reduction of the contents of P for a preceding cycle.

15. (ORIGINAL) A computer program product, comprising a computer readable medium having thereon computer program code means adapted, when said program is loaded onto a computer, to make the computer execute the procedure of any one of claims 1 to 7.